УДК 004.9

ПРОГРАММНАЯ СИСТЕМА АУТЕНТИФИКАЦИИ ПО ДИНАМИКЕ РУКОПИСНОЙ ПОДПИСИ В БАНКОВСКОЙ СФЕРЕ

Э.С. Анисимова,
Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, г. Казань

Ключевые слова: *динамическая рукописная подпись, распознавание, аутентификация, нечёткие признаки.*

На протяжении столетий рукописная подпись человека традиционно используется в качестве метода заверения разного рода договоров и соглашений. Общепринято подпись считается доказательством волеизъявления того или иного человека. Однако, рукописные подписи, сделанные чернилами на бумаге, достаточно затратны в плане времени и ресурсов. Внедрение технологии безбумажного документооборота открыло возможность использовать подписи в электронной форме и вводить их с помощью графического планшета. Переход к электронным рукописным подписям способен снизить риски, удовлетворить требования клиентов и является наименее проблемным для использования в банковской сфере.

Электронная рукописная подпись фиксируется специальным пером на экране графического планшета. Она представляет собой не просто графическое изображение (как обычная статическая подпись, созданная на бумаге), она несёт в себе совокупность биометрических параметров (ускорение, изменение давления, угол наклона пера в процессе записи и т.д.). Поэтому использовать электронную рукописную подпись с целью аутентификации клиентов банка более надёжно и безопасно по сравнению с обычной статической подписью.

В процессе записи в режиме реального времени считываются следующие параметры подписи:

– пространственные координаты конца пера x(t) и y(t),
– давление конца пера на планшет,
– наклон пера,
– угол движения пера.

Системы аутентификации личности по рукописной подписи в разной степени используют те или иные параметры, характеризующие динамику написания подписи.

Каждая из систем обеспечивает определённую эффективность (точность) распознавания подписей. В настоящее время актуальна задача повышения эффективности распознавания рукописных подписей, также актуальна и разработка систем, обеспечивающих более высокую эффективность распознавания рукописных подписей.

Рассмотрим новую программную систему аутентификации по динамике рукописной подписи [1, 4]. Система создаёт для каждого зарегистрированного пользователя эталон подписи, содержащий идентификатор пользователя и совокупность функций принадлежности для нечётких признаков кривизны (площадь криволинейной области, нечёткое количество пиков, относительное количество участков монотонностей, относительная длина участков возрастания, ускорение). Использование нечётких признаков кривизны [3, 6] позволяет формализовать размытый характер подписи (размытость означает тот факт, что даже две подписи одного и того же автора могут существенно различаться). Следует отметить, что построение функций принадлежности осуществляется на основе метода потенциалов (С.Д. Штовба). Метод потенциалов [2] позволяет построить функции принадлежности даже на небольшом количестве значений выборки. И это обстоятельство является весьма удобным при построении системы аутентификации по динамике рукописных подписей, так как запрашиваемое количество подписей пользователя не может быть огромным, что, например, требуют для построения функции принадлежности в статистике. Метод потенциалов осуществляет анализ плотности экспериментальных данных. Для каждого значения признака вычисляется значение потенциала, определяющего, насколько плотно расположены соседние значения признака по отношению к оцениваемому значению.

Значение потенциала pot_i определённой точки (значения) y_i вычисляется следующим образом:

$$pot_i = \sum_{j=1..\nu} e^{-4\alpha^2 (y_i - y_j)^2} \qquad (1)$$

где y_i, y_j - точки (значения признака), α – коэффициент, определяющий степень компактности кластера, ν – количество точек (значений признака).

Далее осуществляется нормализация значений потенциалов:

$$\mu_y(y_i) = \frac{pot_i}{\max\limits_{j=1..\nu}(pot_j)} \qquad (2)$$

и на основе значений потенциалов производится построение функций принадлежности.

При проведении процедуры аутентификации клиент предъявляет свой идентификатор и вводит подпись на экране графического планшета. Далее система считывает последовательности всех динамических параметров, для каждого параметра вычисляет значения нечётких признаков кривизны. После этого осуществляется вычисление степеней принадлежности значений нечётких признаков соответствующим функциям принадлежности, хранящимся в эталоне пользователя с предъявленным идентификатором. Для определения величины сходства введённой подписи с эталоном вычисляется t-норма «произведение», широко используемая в нечёткой логике, – вычисляется произведение степеней принадлежности значений признаков введённой подписи соответствующим функциям принадлежности. Если произведение

степеней принадлежности превышает значение индивидуального порога пользователя, введённая подпись считается подлинной, иначе – поддельной.

Эксперименты по определению эффективности предложенной системы аутентификации по динамике рукописной подписи были проведены на коллекции подписей MCYT_Signature_100 [7]. Эта коллекция включает подписи 100 пользователей, для каждого из которых взято по 25 подлинных и 25 поддельных подписей. На рисунке 1 представлено несколько подлинных подписей одного из пользователей коллекции MCYT_Signature_100.

Рис. 1. Образцы подлинных подписей пользователя MCYT_Signature_100

Обучение системы распознавания проводилось на 20 подлинных подписях каждого клиента коллекции, т.е. на наборе из 20 х 100 = 2000 подлинных подписей.

Тестирование проводилось на оставшихся 5 подлинных подписях и 25 умелых подделках подписей 100 зарегистрированных пользователей, т.е. на наборе из 500 подлинных подписей и 2500 умелых подделок подписей.

Результаты проведенных экспериментов показали достаточно высокую эффективность предложенной системы аутентификации: средняя величина FRR составила 3 %, FAR – 1 %, что значительно превосходит результаты многих современных программных систем [5, 8]. В этой связи предложенная система аутентификации по динамике рукописной подписи может быть успешно применена в банковской сфере для проведения операций с розничными клиентами.

Список литературы

1. *Аникин И.В., Анисимова Э.С.* Распознавание рукописных подписей на основе нечетких признаков и метода потенциалов // Информация и безопасность. 2016. № 4 (4). С. 567–570.

2. *Штовба С.Д.* Введение в теорию нечетких множеств и нечеткую логику [Электронный ресурс].

URL: http://matlab.exponenta.ru/fuzzylogic/book1/13_3.php (дата обращения: 24.02.2017).

3. *Anikin I.V.* Document New type of takagi-sugeno fuzzy inference system as universal approximator // Applied Mechanics and Materials. 2014. Vol. 598. P. 453–458.

4. *Anikin I.V., Anisimova E.S.* Handwritten signature recognition method based on fuzzy logic // Dynamics of Systems, Mechanisms and Machines (Dynamics). 2016. P. 1–5.

5. *Cpalka K.* New method for on-line sig-nature verification based on horizontal partitioning // Pattern Recognition. 2014. Vol. 47. P. 2652–2661.

6. *Glova V.I.* Method for Recognition of Fuzzy 2D Primitives via a Technology of Soft Computing // Pattern Recognition and Image Analysis. 2001. Vol. 11(1). P. 164–167.

7. *Ortega-Garcia J.* MCYT baseline corpus: a bimodal biometric database // IEE Proc.Vis. Image Signal Process. 2003. Vol. 150(6). P. 395–401.

8. Qiao Y. Learning Mahalanobis distance for DTW based online signature verification // IEEE International Conference on Information and Automation (ICIA). 2011. P. 333–338.